(12) UK Patent Application (19) GB (11) 2 369 205 (13) A

(43) Date of A Publication 22.05.2002

(21) Application No 0028154.3

(22) Date of Filing 17.11.2000

(71) Applicant(s)
DATAWIPE MANAGEMENT SERVICES LTD
(Incorporated in the United Kingdom)
Unit A, Cromwell Road, CAMBERLEY, Surrey, GU15 4HY, United Kingdom

(72) Inventor(s)
Philip John Hayward

(74) Agent and/or Address for Service
Wildman Harrold Allen & Dixon
11th Floor Tower 3, Clements Inn, LONDON, WC2A 2AZ, United Kingdom

(51) INT CL[7]
G06F 12/14

(52) UK CL (Edition T)
G4A AAP

(56) Documents Cited
US 6026293 A

(58) Field of Search
UK CL (Edition S) G4A AAP AUXX
INT CL[7] G06F 1/00 12/14 13/38 , H04Q 7/32
ONLINE:WPI,EPODOC,JAPIO US Class 700/231, 700/237,711/100,711/164

(54) Abstract Title
Personal data device and protection system with deletion of contents

(57) A personal data device have a memory for storing personal data and a data storage and processing module for enabling operation of the device and a two part code for enabling access to the data where a first part of the code is stored in the memory of the device and second part of the code is stored in the data storage and processing module, such that when the two parts of the code do not correspond, the personal data in the memory is deleted. A database server may be provided for maintaining a copy of the data stored on the personal data device so that deleted data can subsequently be reloaded.

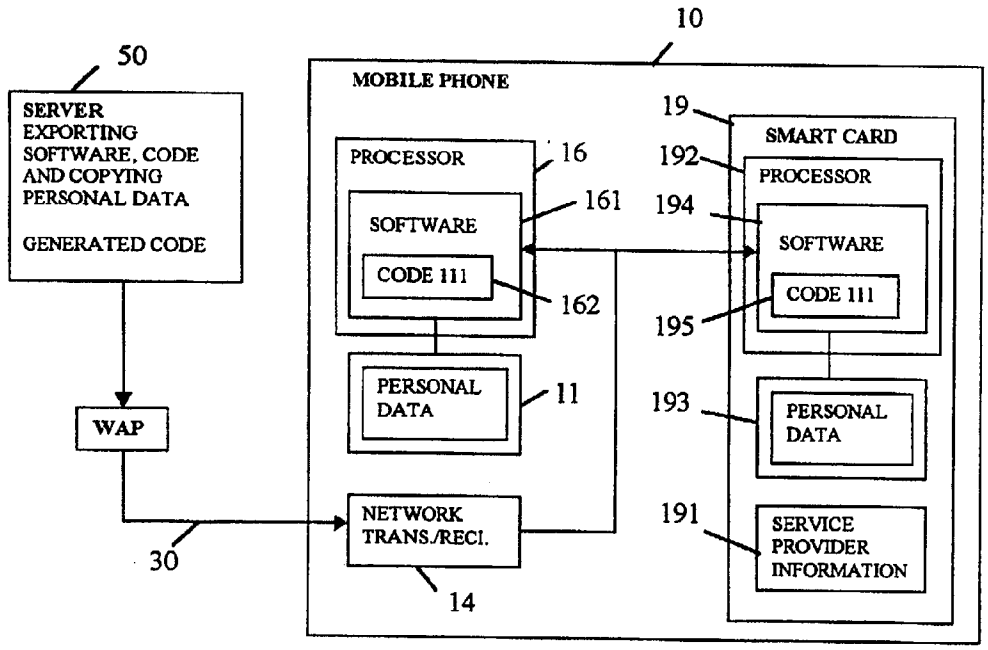


Fig. 1A

GB 2 369 205 A

The claims were filed later than the filing date but within the period prescribed by Rule 25(1) of the Patents Rules 1995.

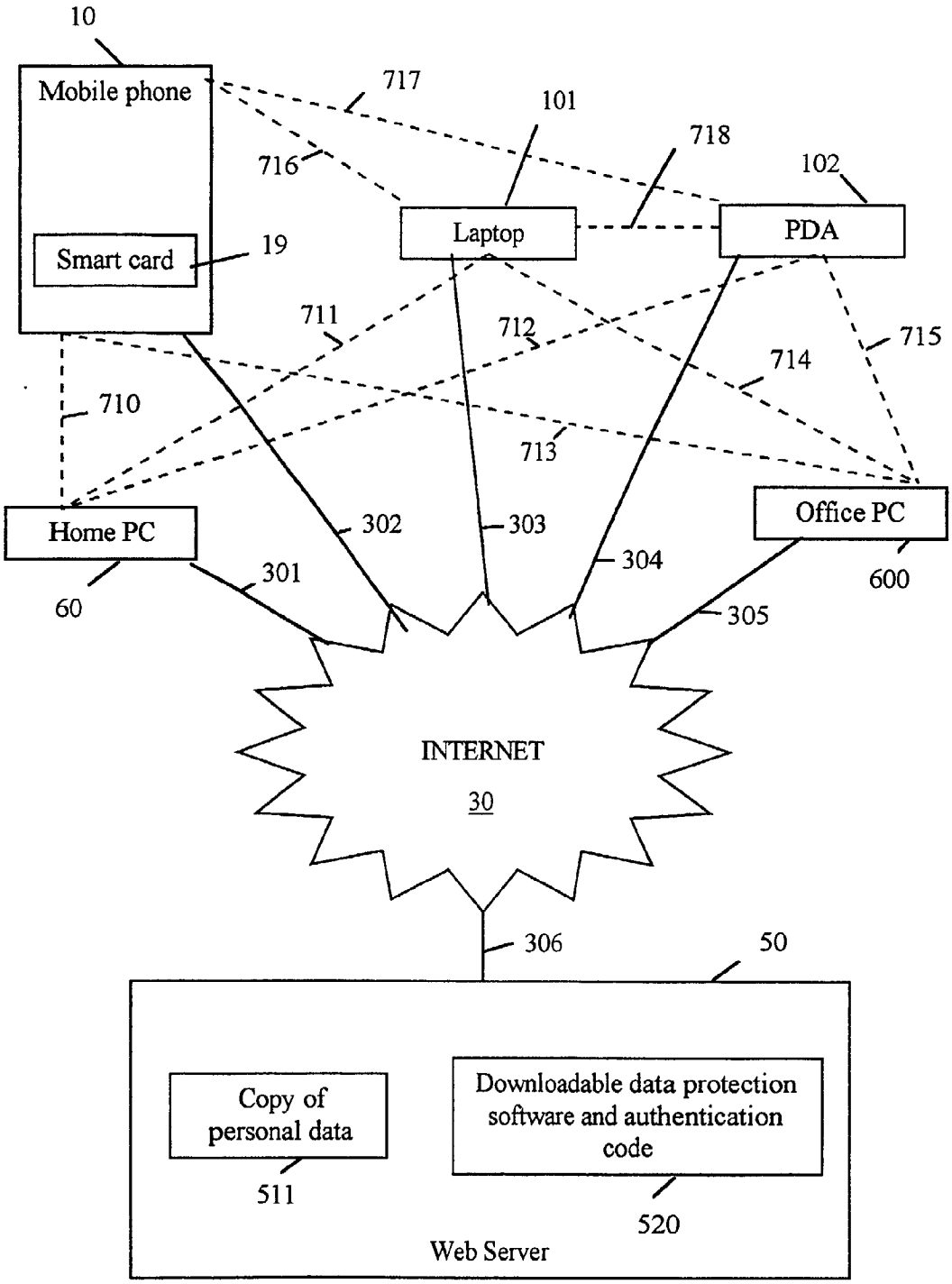

10
Mobile phone
717
101
718
716
102
Laptop
PDA
Smart card
19
711
712
715
714
710
713
Home PC
302
303
Office PC
304
301
600
60
305
INTERNET
30
306
50
Copy of personal data
Downloadable data protection software and authentication code
511
520
Web Server

Fig. 1

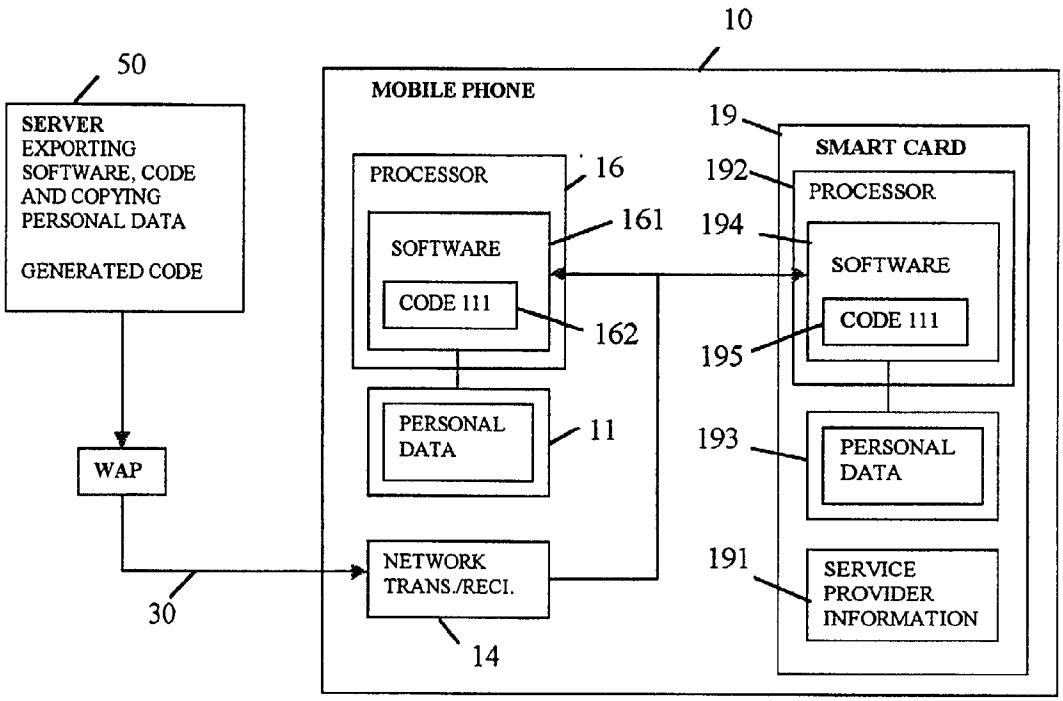

10
50
SERVER
EXPORTING
SOFTWARE, CODE
AND COPYING
PERSONAL DATA
GENERATED CODE
MOBILE PHONE
19
SMART CARD
PROCESSOR
16
192
PROCESSOR
161
194
SOFTWARE
SOFTWARE
CODE 111
CODE 111
162
195
PERSONAL
DATA
11
193
PERSONAL
DATA
WAP
NETWORK
TRANS./RECI.
191
SERVICE
PROVIDER
INFORMATION
30
14

Fig. 1A

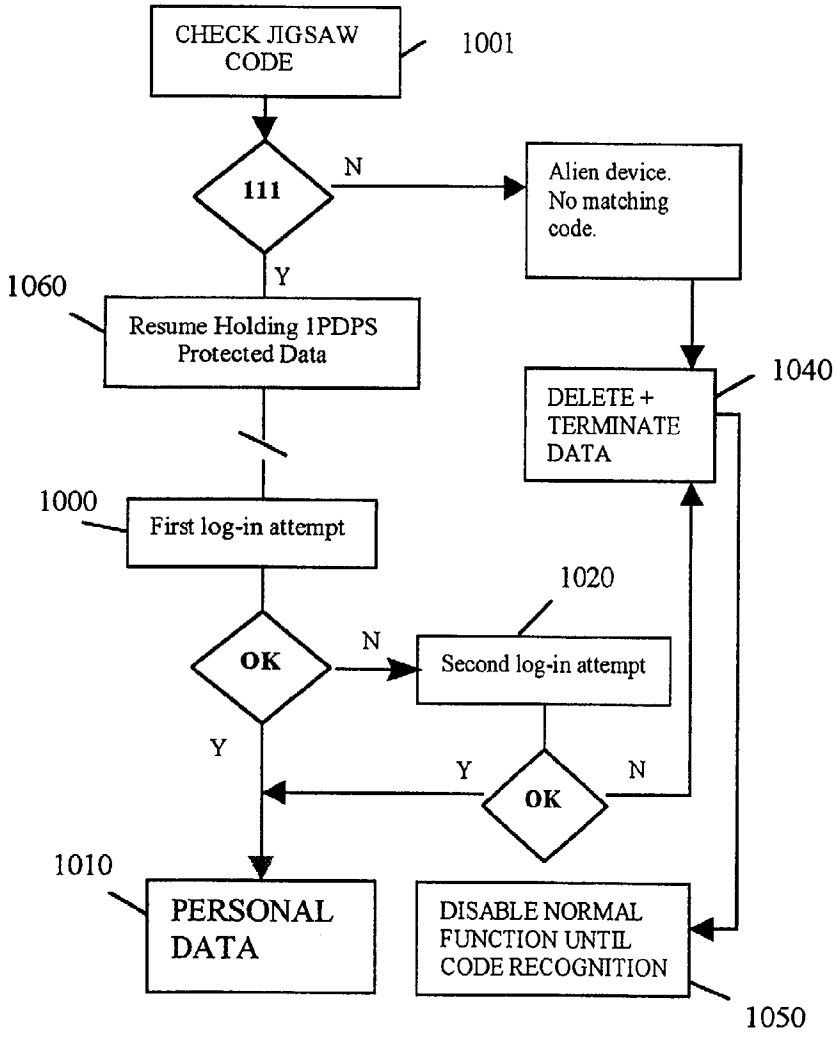

CHECK JIGSAW CODE
1001
111
N
Alien device. No matching code.
Y
1060
Resume Holding 1PDPS Protected Data
1040
DELETE + TERMINATE DATA
1000
First log-in attempt
1020
OK
N
Second log-in attempt
Y
Y
N
OK
1010
PERSONAL DATA
DISABLE NORMAL FUNCTION UNTIL CODE RECOGNITION
1050

Fig. 1B

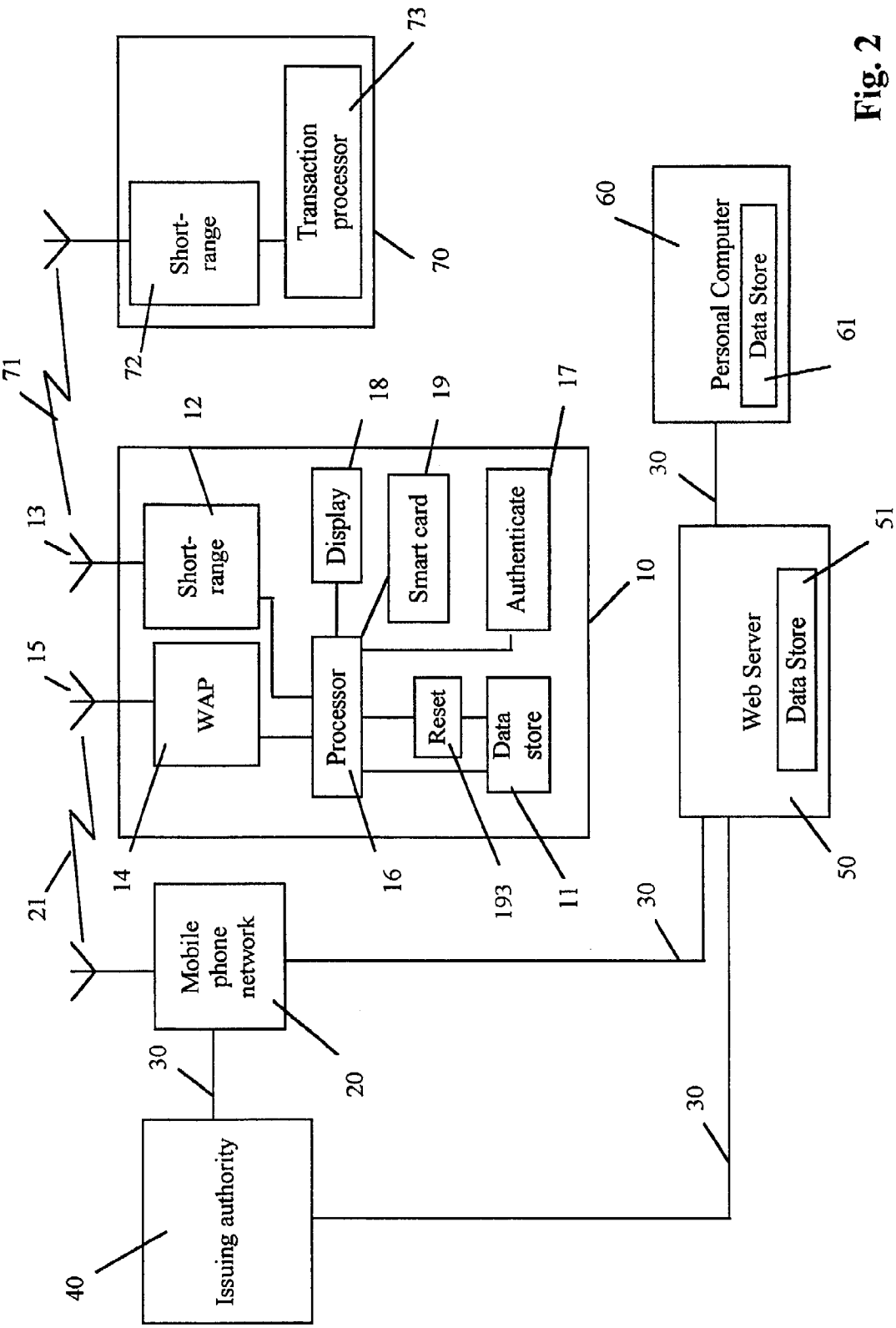

Short-range
Transaction processor
73
70
72
71
12
18
19
17
Display
Smart card
Authenticate
Short-range
13
WAP
15
Processor
Reset
Data store
10
14
16
193
11
21
Mobile phone network
20
30
Issuing authority
40
Personal Computer
Data Store
60
61
30
Web Server
Data Store
51
50
30

Fig. 2

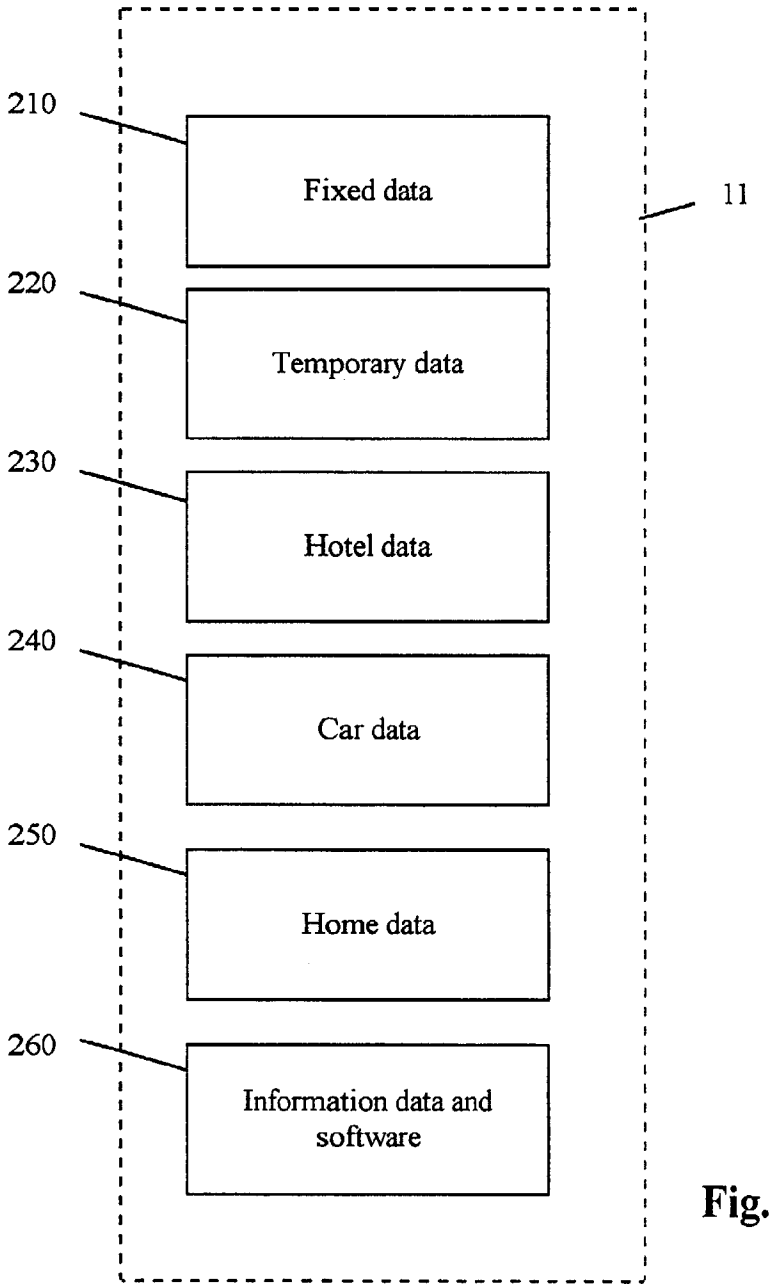

210
Fixed data
11
220
Temporary data
230
Hotel data
240
Car data
250
Home data
260
Information data and software

Fig. 3

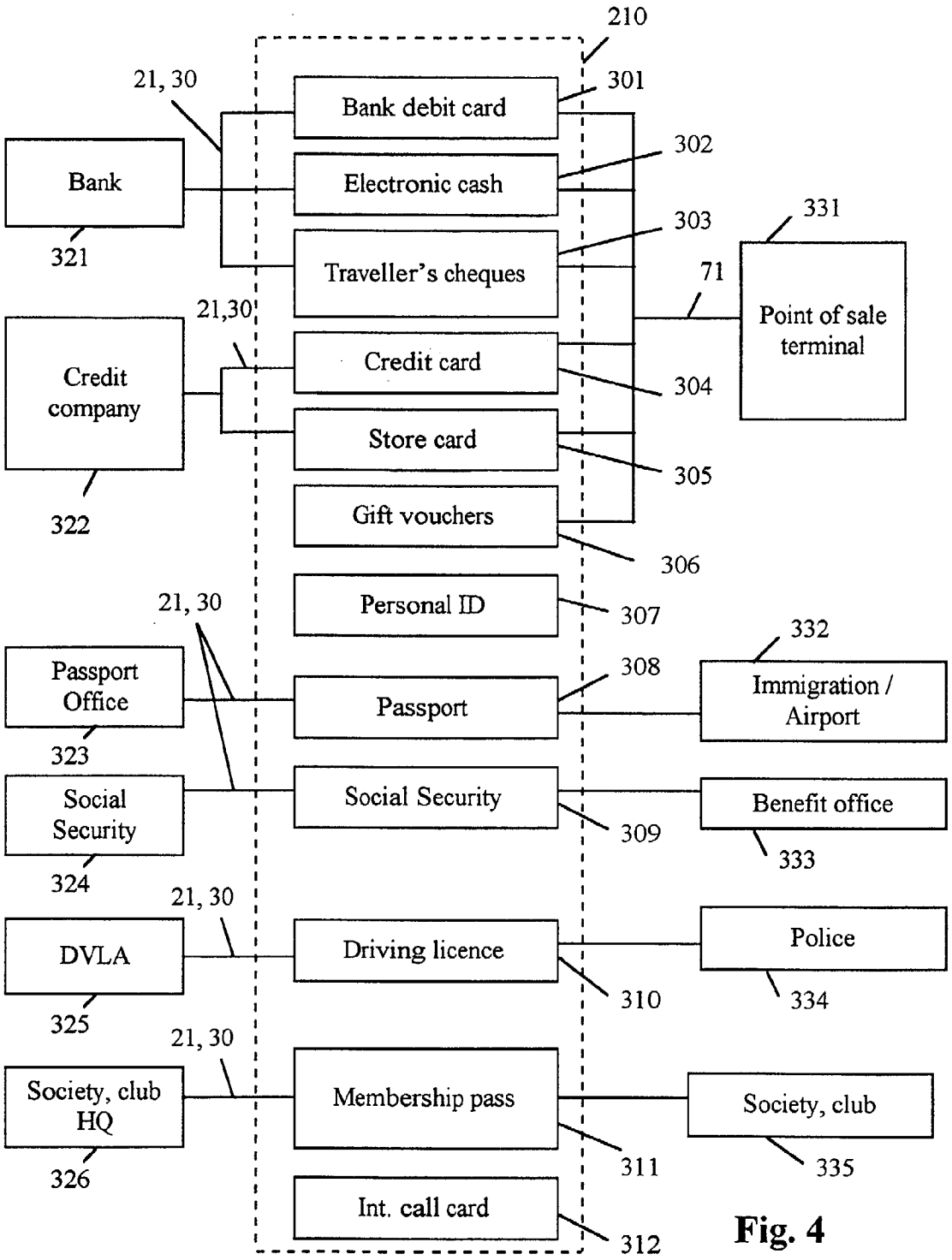

210
21, 30
301
Bank debit card
Bank
302
Electronic cash
321
303
331
Traveller's cheques
71
Point of sale terminal
21,30
Credit card
Credit company
304
Store card
305
322
Gift vouchers
306
Personal ID
307
21, 30
332
Passport Office
308
Passport
Immigration / Airport
323
Social Security
Social Security
Benefit office
309
324
333
21, 30
DVLA
Driving licence
Police
310
325
334
21, 30
Society, club HQ
Membership pass
Society, club
311
326
335
Int. call card
312

Fig. 4

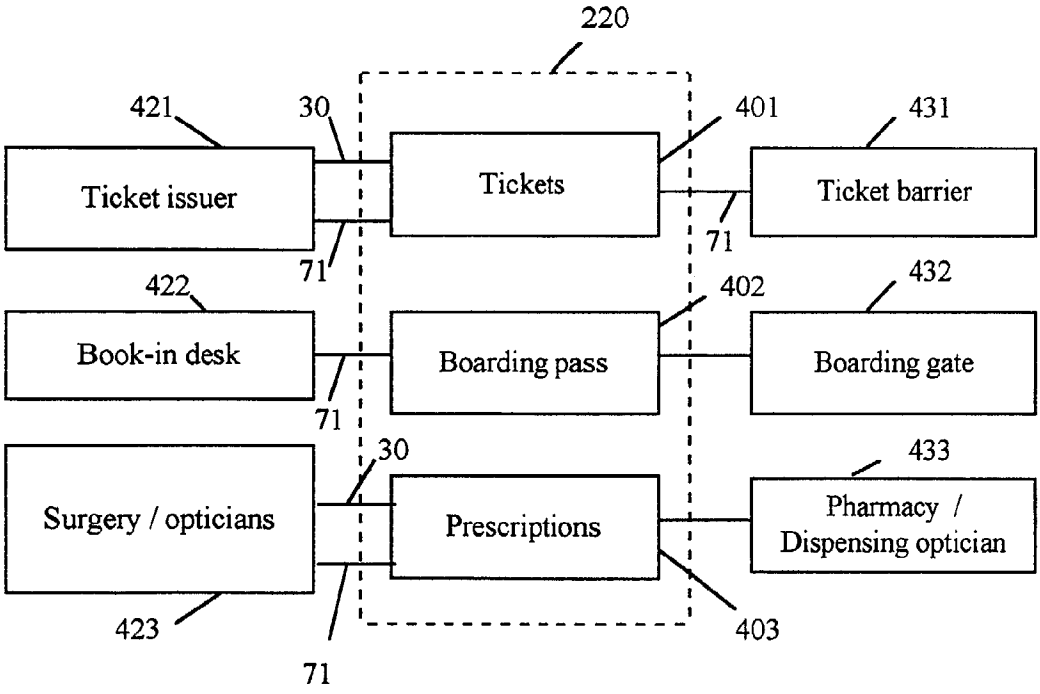

220
421
30
401
431
Ticket issuer
Tickets
Ticket barrier
71
71
422
402
432
Book-in desk
Boarding pass
Boarding gate
71
30
433
Surgery / opticians
Prescriptions
Pharmacy /
Dispensing optician
423
403
71

Fig. 5

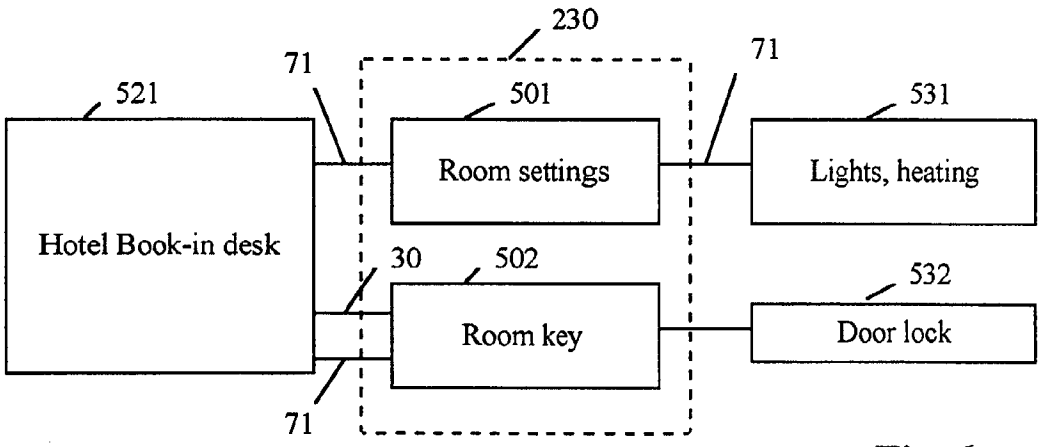

230
71
71
521
501
531
Hotel Book-in desk
Room settings
Lights, heating
30
502
532
Room key
Door lock
71

Fig. 6

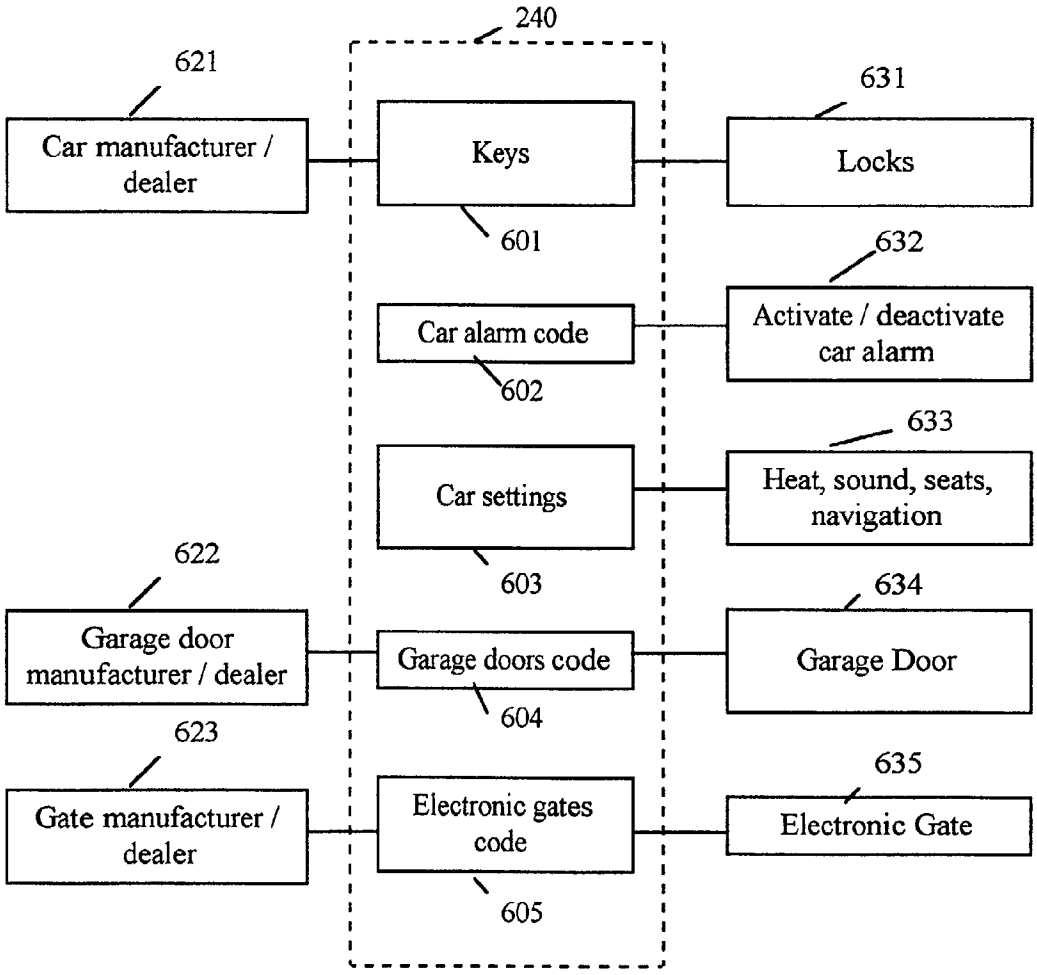

240
621
Car manufacturer / dealer
Keys
601
631
Locks
632
Activate / deactivate car alarm
Car alarm code
602
633
Heat, sound, seats, navigation
Car settings
603
622
Garage door manufacturer / dealer
Garage doors code
604
634
Garage Door
623
Gate manufacturer / dealer
Electronic gates code
605
635
Electronic Gate

Fig. 7

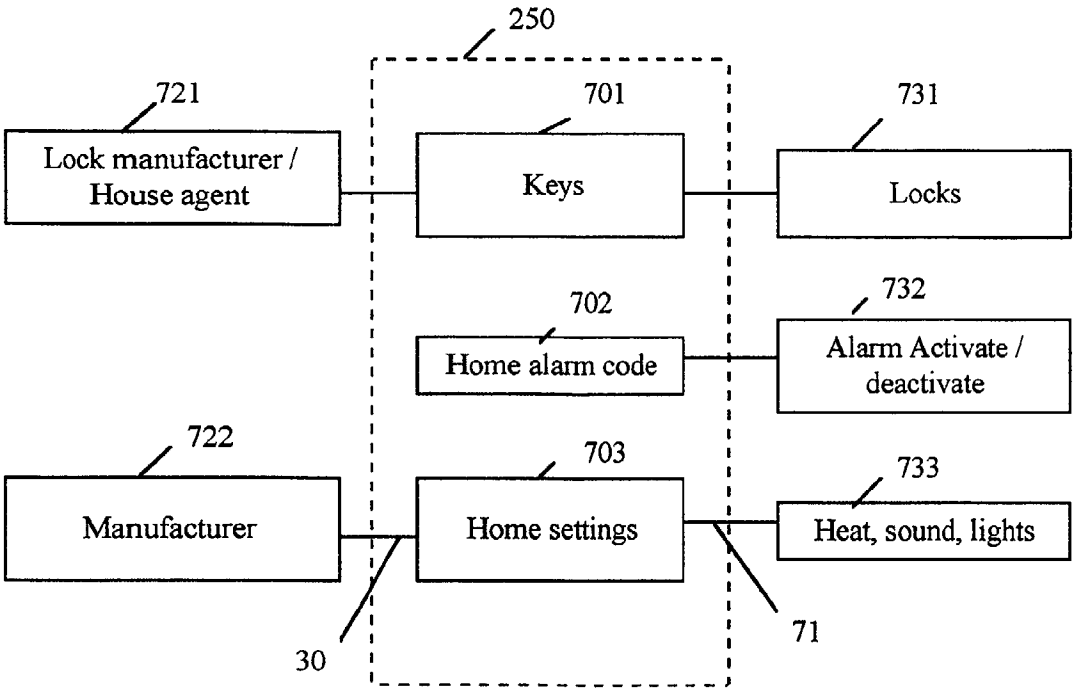

250
721
Lock manufacturer / House agent
701
Keys
731
Locks
702
Home alarm code
732
Alarm Activate / deactivate
722
Manufacturer
703
Home settings
733
Heat, sound, lights
30
71

Fig. 8

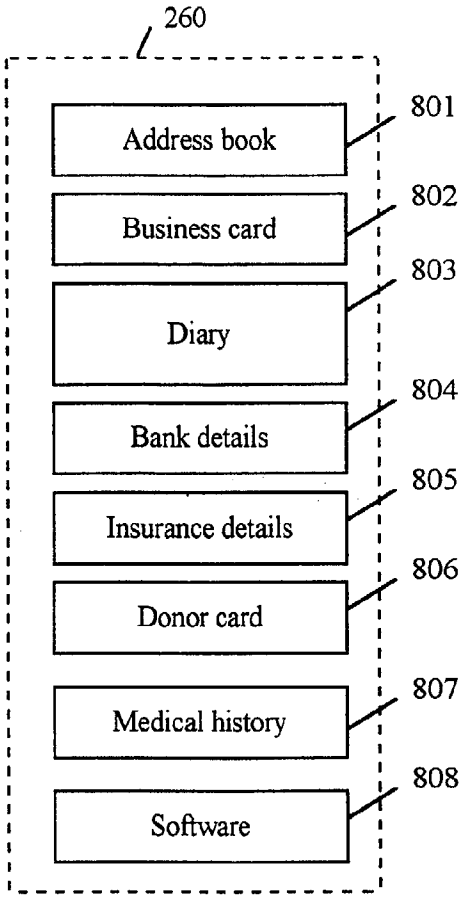

260
Address book
801
Business card
802
Diary
803
Bank details
804
Insurance details
805
Donor card
806
Medical history
807
Software
808

Fig. 9

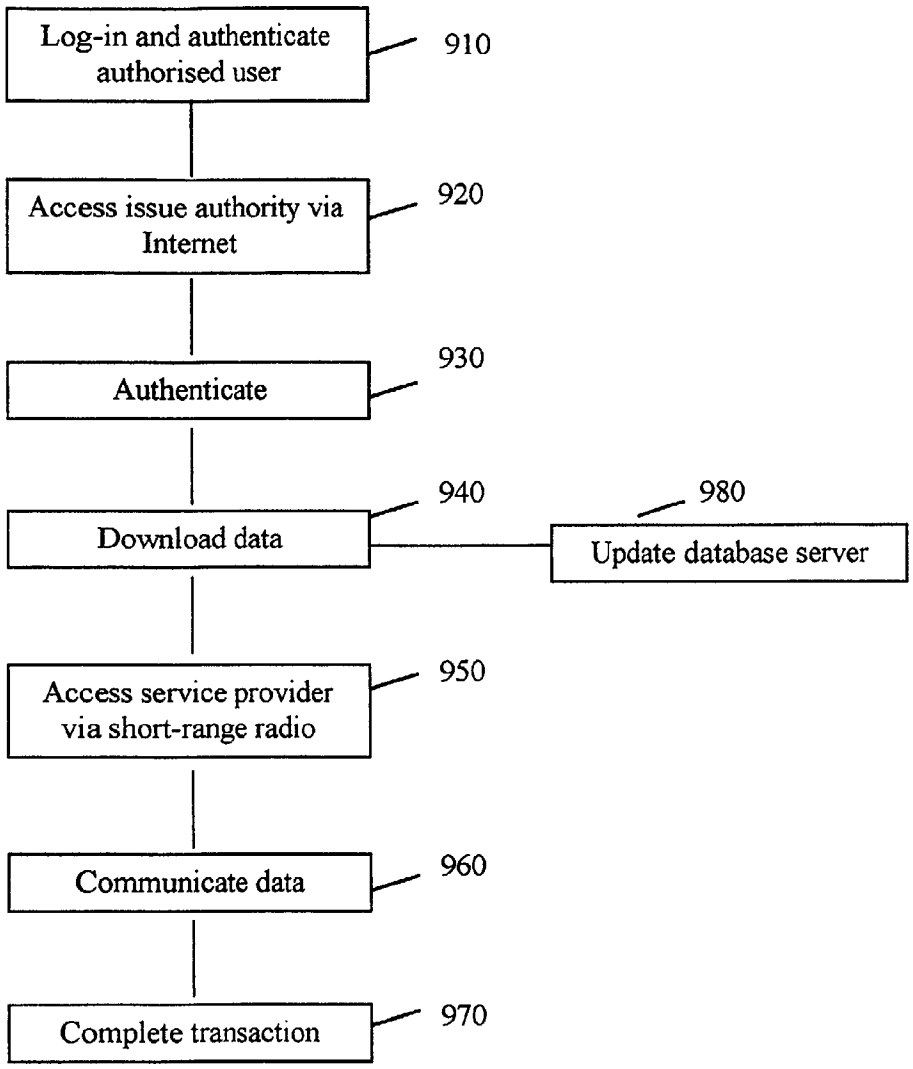
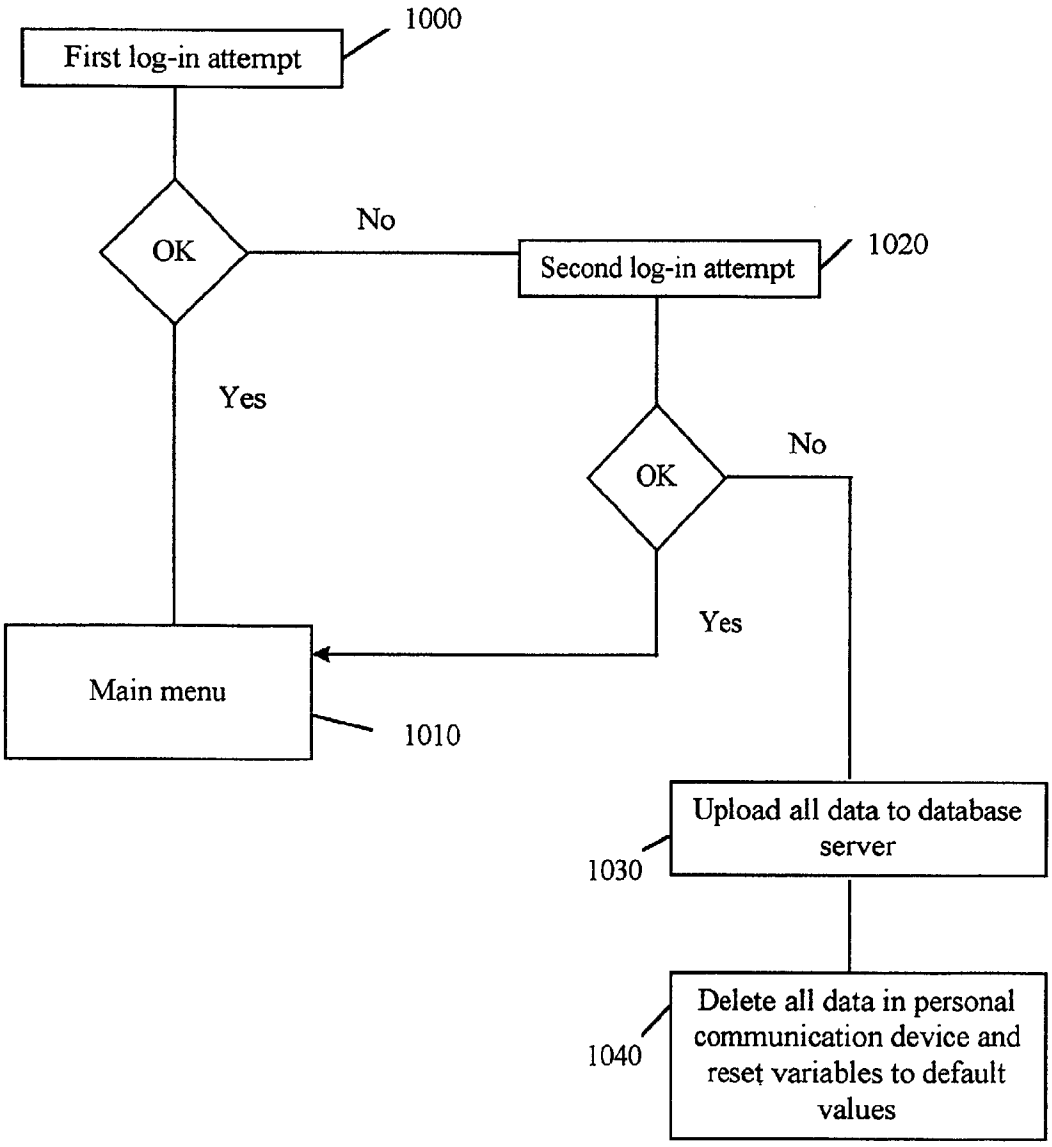

Log-in and authenticate authorised user
910
Access issue authority via Internet
920
Authenticate
930
Download data
940
980
Update database server
Access service provider via short-range radio
950
Communicate data
960
Complete transaction
970

Fig. 10

Fig. 11


First log-in attempt
1000
OK
No
Second log-in attempt
1020
Yes
OK
No
Yes
Main menu
1010
Upload all data to database server
1030
Delete all data in personal communication device and reset variables to default values
1040

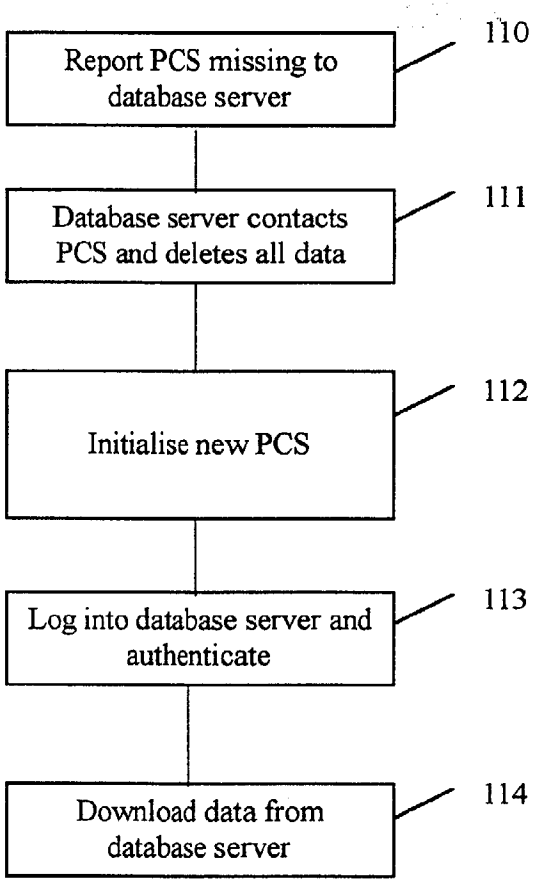

Report PCS missing to database server
110
Database server contacts PCS and deletes all data
111
Initialise new PCS
112
Log into database server and authenticate
113
Download data from database server
114

Fig. 12

PERSONAL DATA DEVICE AND PROTECTION SYSTEM AND METHOD FOR STORING AND PROTECTING PERSONAL DATA

The present invention relates to personal data storage and protection.

Personal data devices, for example digital personal assistants, are known for storing personal data, for example, to act as personal organisers. However, in order to use the stored data the data has to be displayed on a display and to be manually read out or re-keyed into another device. There are proposals to use short-range radio communications in such devices for communicating with, for example, computer peripherals. For example, so-called Bluetooth technology has been proposed for use for communicating with point of sale terminals, for loading money into electronic wallets, for automatic checking-in at hotels and airports, for payment in stores and restaurants, for remote switching on and off of lights and heating and remote locking of doors. Bluetooth is a global standard using a 2.4 GHz frequency band, working over a typical range of up to 100 metres. However, such applications in relation to a personal data device are susceptible to misuse and the requirement for securely protecting the personal data and/or electronic signatures stored in the device becomes more important. In additional, personal data may be stored in, for example, mobile phones and laptop computers and home or office personal computers.

It is an object of the present invention to provide greater security of such stored personal data.

According to a first aspect of the invention there is provided a personal data device including data storage means for storing personal data, access authentication means for restricting access to the personal data stored in the data storage means to an authorised user, a data storage and processing module for enabling operation of the personal data device, data protection software and a synchronisation authentication code, at least a first element of the code being stored in the data storage means and at least a second element of the code being stored in the data storage and processing module, such that, when the at least a first element of the code stored in the data storage means and the at least a second

element of the code stored in the module correspond, access is allowed by the data protection software to the personal data and, when the at least a first element of the code stored on the module and the at least a second element of the code stored in the data storage means do not correspond, the personal data and/or any electronic signatures stored in the data storage means are deleted by the data protection software

Preferably, the personal data device further includes first communication means for downloading the data protection software and the synchronisation authentication code from a remote server.

Alternatively, the data protection software and the synchronisation authentication code are downloadable from the data storage and processing module.

Preferably, the first communication means is also for communicating with the remote server or another computer device for transmitting a copy of the personal data to the remote server or other computer device such that synchronisation of the personal data with the data stored on the server or other computer device is permitted by the data protection software dependant upon authentication with the server or other computer device using the synchronisation authentication code.

Advantageously, personal data and/or electronic signatures may also be stored in the data storage and processing module.

Conveniently, the access authentication means permits access to the personal data in response to a predetermined input and in response to a consecutive input a predetermined number of times of an input other than the predetermined input the data protection software deletes any personal data and/or electronic signatures stored in the data storage means and in the data storage and processing module.

Conveniently, the access authentication means includes pattern recognition means.

Advantageously, the pattern recognition means is for recognising at least one of the authorised user's fingerprint pattern, iris pattern and voice pattern.

Conveniently the data storage and processing module is removable from the personal data device.

Advantageously, the data storage and processing module is a smart card.

Preferably, the personal data device includes deletion means under control of the data protection software for deleting personal data stored in the data storage means and the data storage and processing module when an input to the access authentication means does not match the predetermined input.

Preferably, the deletion means is also for deleting the personal data and/or electronic signatures, under control of the data protection software, on receipt of a deletion signal from the remote server.

Advantageously, the deletion signal from the remote server is an SMS message.

Advantageously, the personal data device is provided with uninterruptible standby power supply means sufficient to power the first communication means for reception of the deletion signal and to power the deletion means to delete the personal data and/or any electronic signatures.

Conveniently, the deletion means is also for resetting variables stored in the personal data device to default values.

Conveniently, the personal data device includes means for establishing communications with the database server to synchronise personal data stored in the data storage means with personal data stored on the server after a predetermined number of additions or amendments to the stored data have been made.

Preferably encryption means are provided for storing the personal data on the personal data device in an encrypted form.

Conveniently, the personal data device further includes second communication means for transferring at least some of the stored personal data between the personal data device and a transaction terminal.

Preferably, the first communication means is for connection to a mobile communications network and the second communication means is a short-range wireless communication means.

Conveniently, the short-range wireless communication means is adapted to operate over a range up to 100 metres.

Preferably, the personal data device storage device includes display means and the device is adapted to display appropriate menu items or icons on the display means dependent on detection of a signal transmitted from a transaction terminal within range of the short-range wireless communication means.

Preferably, the personal data device data storage means is for storing fixed data updatable only be a corresponding issuing authority and for storing user data updatable by the authorised user.

Conveniently, the personal data device data storage means is for storing data corresponding to any one or more of a credit card, a debit card, a passport and social security data .

Preferably, the personal data device data storage means is for storing electronic cash and/or travellers' cheques.

Preferably, the personal data device data storage means is for storing temporary data updatable by an issuing authority, including any one or more of tickets, boarding passes, prescriptions and hotel room access keys.

Preferably, the personal data device data storage means is for storing data relating to the authorised user's home and/or car, including any one or more of access keys, alarm control, automatic door and gate control.

Preferably, the personal data device data storage means is for storing user-updatable data including any one or more of address book entries, business cards, appointment diary, bank details, insurance details, donor card and medical history.

According to a second aspect of the invention there is provided a database server including server data storage means, downloadable data protection software and an authentication code generator, and server communication means for downloading to first communication means on a personal data device including data storage means for storing personal data and a data storage and processing module for enabling operation of the personal data device, data protection software and a synchronisation authentication code for storing at least a first element of the code in the data storage means and at least a second element of the code in the data storage and processing module, and for receiving from the personal data device a copy of the personal data for storing in the server data storage means dependant upon authentication using the synchronisation authentication code, such that, when the first element of the code stored in the module and the second element of the code stored in the data storage means correspond, access is allowed by the data protection software to the personal data and synchronisation of the personal data with the data stored on the server is permitted by the data protection software and, when the first element of the code stored on the module and the second element of the code stored in the data storage means do not correspond, the personal data and/or any electronic signatures stored in the personal data device data storage means is deleted by the data protection software.

Preferably, the database server includes data comparison means for comparing a first version of the personal data uploaded from the personal data device and a second version of the personal data stored in the server data storage means and means to extract a current version of the data from the first version and the second versions from which to form a synchronised version to replace the data stored on both the personal data device and the database server.

Preferably the database sever includes encryption means and decryption means such that the personal data may be stored in the server data storage means in an encrypted format.

Conveniently, the database server is provided with signalling means to communicate with the personal data device to signal the deletion means to delete the personal data and/or any electronic signatures in the personal data device data storage means.

Preferably the signalling means is for signalling the personal data device to delete the personal data and/or any electronic signatures stored in the personal data device data storage means on the database server being updated that the personal data device is no longer in the possession of the authorised user.

Advantageously, replacement means are provided to replace a personal data device that has been reported lost or stolen with a replacement personal data device into which the personal data stored on the database server may be reloaded.

According to a third aspect of the present invention, there is provided a personal data protection system comprising:

a personal data device including data storage means for storing personal data, a processing and data storage module for enabling operation of the personal data device when a first element of a synchronisation code stored in the module corresponds with a second element of the authentication code stored in the data storage means, first communication means for connection of the personal data device to a communication network; and

a database server including server communication means connectable to the communications network for downloading a copy of the personal data stored in the personal data device, server data storage means for storing the copied data, such that the data in the database server and the data in the personal data device may be mutually updated and synchronised by communication over the communications network, downloadable data protection software for downloading to the personal data device and a synchronisation code generator for generating a synchronisation code for downloading to the personal data device.

Preferably, the personal data device is further provided with short-range wireless communication means for communicating at least some of the personal data and the system is further provided with a transaction terminal having short-range wireless communication means for communicating with the short-range communications means of the personal data device for initiating a transaction by the transaction terminal.

Preferably, the system is further provided with an issuing authority server having issuing authority communication means for updating the personal data stored in the personal data device.

Conveniently, the issuing authority server is connectable to the communications network for updating the personal data stored in at least one of the database server and the personal data device.

Alternatively, or in addition, the issuing authority server includes short-range issuing authority communication means for communicating with the personal data device short-range communication means for updating the personal data stored in the personal data device.

According to a fourth aspect of the present invention there is provided a method for storing and protecting personal data comprising the steps of:

a) providing a personal data device including data storage means for storing personal data, first communication means for communicating over a communications network and a data processing and storage module for enabling operation, under control of data protection software, of the personal data device when a first element of a synchronisation code stored on the module corresponds with a second element of a synchronisation authentication code stored in the personal data device storage means;

b) storing personal data in the data storage means;

c) providing a database server connectable to the communications network for receiving from the personal data device and storing a copy of the personal data stored in the personal data device such that the personal data in the personal data device and the database server may be mutually updated and synchronised;

d) providing downloadable data protection software and a synchronisation authentication code generator on the database server;

e) downloading the data protection software and a synchronisation code from the database server to the personal data device and loading a first element of the synchronisation authentication code in the data storage and processing module and a second element in the data storage means of the personal data device such that operation of the personal data device is enabled;

f) providing deletion means in the personal data device for deleting, under control of the data protection software, the personal data and/or electronic signatures stored in the data storage means when the first element of the synchronisation code does not correspond with the second element of the synchronisation authentication code or on receipt of a deletion signal from the database server.

According to a fifth aspect of the invention there is provided a computer program comprising code means for performing all the steps of the method described above when the program is run on one or more computers.

Advantageously, the computer program is embodied on a computer-readable medium.

According to a sixth aspect of the invention there is provided a computer program product comprising program code means stored in a computer-readable medium for performing the method described above when that program product is run on one or more computers.

A specific embodiment of the invention will now be described by way of example with reference to the accompanying drawings, in which:

Fig. 1 shows a schematic block diagram of the system for protecting personal data according to the present invention;

Fig 1A shows a schematic block diagram of a mobile telephone and server of Fig. 1;

Fig 1B shows a flowchart of the use of the synchronisation authentication code used in the present invention.

Fig. 2 shows a schematic block diagram of an embodiment of the system of Fig. 1 in relation to a personal data device;

Fig. 3 shows groups of personal data stored in the personal data device used with the system of Fig. 2;

Fig. 4 shows fixed data of Fig. 3, and examples of sources and recipients for downloading and uploading the fixed data respectively;

Fig. 5 shows temporary data of Fig. 3, and examples of sources and recipients for downloading and uploading the temporary data respectively;

Fig. 6 shows hotel data of Fig. 3, and examples of downloading and uploading the hotel data;

Fig. 7 shows car data of Fig. 3, and examples of downloading and uploading the car data;

Fig.8 shows home data of Fig. 3, and examples of downloading and uploading the home data;

Fig. 9 shows information data of Fig. 3;

Fig. 10 is a flowchart showing the method of downloading data to and communicating data from the personal data device used with the system shown in Fig. 2;

Fig. 11 is a flowchart of the logging in step of the method of Fig. 10;

Fig. 12 is a flowchart of the procedure followed when a personal data device of the system of Fig. 2 is found to be missing.

In the figures, like reference numerals denote like parts or steps.

The system of the invention as shown in Fig. 1 includes a web server 50 connected to the Internet 30 by a connection 306. The web server includes downloadable data protection software and a generator for generating downloadable authentication codes 520. Also connectable to the Internet are a number of devices, belonging to the same user, which may contain personal data. These include a mobile telephone or personal data device 10 connectable by a connection 302, a laptop computer 101 connectable by a connection 303, a PDA (personal data administrator) 102 connectable by connection 304, a home PC 60 connectable by a connection 301 and an office PC 600 connectable by a connection 305. By means of the said connections, the personal data stored on

each or any of these devices may be downloaded onto the web server where a copy of the personal data file 11 (see Fig 1A) may be stored. By comparing the data stored in each of the devices with the copy of the data stored on the web server, an up-to-date version of the personal data can be maintained on the web server and the data synchronised with the data on each of the other devices. In addition, the mobile telephone 10, for example, may communicate by short range radio communications using, for example, Bluetooth protocol with any of the other devices within range. In this manner the data held on a home PC 60 and on the mobile telephone 10 can be synchronised by means of the radio link 710. In the same way, data held on the mobile telephone 10 may be synchronised with the PDA 102 via the link 717, with the laptop computer 101 via link 716 and with an office PC 600 via a link 713. Similarly data on the computer laptop may be synchronised via link 711 with data on the PC 60 and with the PDA 102 by a link 718, when these devices are within range. In a similar manner, the data on the office PC 600 can be synchronised with the laptop 101 over link 714 and with the PDA 102 over link 715. In this manner, the data on any of the portable devices 10, 101, 102 may be synchronised with the data on either of the home PC 60, or the office PC 600, whenever the devices are within range of the PCs and the data held on the portable devices may be synchronised with each other whenever they are within range of each other. In addition, by connecting any of the devices to the Internet, the data can be synchronised with the data held on the web server 50.

Instead of using short range wireless communications between the portable devices and the PCs, they may be linked by, for example, hardwiring or infrared communications.

Authentication codes and data protection software can be downloaded from the web server 50 to any of the authorised user's devices via the Internet 30. This means the data can be protected from misuse in a manner to be described and synchronisation can be restricted to devices belonging to the same user. For fuller protection, all of the devices may be provided with smart cards, so that the data protection software provides access to the personal data on any of the devices only when an element of the synchronisation authentication code on the smart card corresponds with an element of the synchronisation authentication code stored in

the device and synchronisation of personal data is permitted only between devices having corresponding synchronisation authentication codes. In an embodiment of the invention, the data protection software and authentication code may alternatively be downloaded into the personal data device from the smart card or be processed by the smart card.

An implementation of an aspect of the invention in relation to a mobile telephone is shown in Fig. 1A. The mobile telephone 10 includes a smart card 19, a processor 16, a data store 11 for personal data and a transmitter/receiver 14 for WAP communications. The mobile telephone is connectable using WAP protocol via the internet 30 to a web server 50. The smart card includes known mobile telephone service provider information 191 for normal operation of the mobile telephone. Also included in the smart card are a known processor 192 and a known data store 193 which may include personal data, for example, telephone numbers and/or electronic signatures.

As indicated in Fig. 1A, data protection software 161 may be downloaded from the web server 50 and a first element 161 of the software loaded into the mobile telephone processor 16 and a second element 194 of the software loaded into the smart card. Similarly, a synchronisation authentication code unique to a particular user can be generated in the web server 50 and downloaded to the mobile telephone 10, so that a first element 162 of the code is accessible to the mobile telephone processor 16 and a second element 195 of the code is stored on the smart card and is available to the smart card processor 192.

As shown in Fig. 2, the system of one aspect of the invention includes a personal data device 10 including a data store 11 accessible by a processor 16. Also connected to the processor is a short-range radio communications transmitter/receiver 12, connected to a first radio antenna 13, and a mobile telephone transmitter/receiver 14 connected to a second radio antenna 15. The mobile telephone transmitter/receiver 14 is adapted to use a mobile telephone network 20 over a radio link 21 to access an Internet network 30. It will be understood that the antennas 13 and 15 may be combined into a single antenna. Also connected to the processor is an authentication module 17, a display 18 and a reset facility 193.

By means of the Internet 30, the personal data device 10 may be connected to an issuing authority web-site server 40 or a web-site database server 50. The database server 50 is provided with a data store 51.

The database web-site server is also connectable by the Internet 30 to a personal computer 60 having a data store 61.

Using the short-range radio transmitter/receiver 12, the personal data device 10 may also be in radio communication over a radio link 71 with a transaction terminal 70 equipped with a compatible short-range transmitter/receiver 72 in communication with a transaction processor 73 within the transaction terminal.

The short-range transmitter/receivers 12, 72 may conveniently use the known so-called Bluetooth protocol.

As shown in Fig. 3, the personal data device data store 11 may include groups of data as follows: fixed data 210, temporary data 220, hotel data 230, car data 240, home data 250 and information data and software 260. These types of data are given for illustration only and one or more such grouping or different groupings may be used. Moreover, the method of organisation of the data does not form part of the invention and any convenient known method of organising the data may be used. Furthermore, the physical data storage means used for storing the data is irrelevant to the invention.

Preferably encryption/decryption facilities are provided such that the data may be stored in an encrypted format.

The fixed data 210 is shown in greater detail in Fig. 4, which shows examples of the types of fixed data 301-312, such as debit card details 301, that may be held. This data is obtained from issuing authorities 321-326 and the data is used to obtain services from service providers 331-335 in a manner to be described.

The temporary data 220 stored in the personal data device 10 is shown in greater detail in Fig. 5, with examples of data relating to a ticket 401, a boarding

pass 402 and a prescription 403 with indications of the respective issuing authorities 421-423 and the service providers 431-433.

An example of hotel data 230 stored in the personal data device 10 is shown in Fig. 6, namely room settings data, such as lighting and heating remote control codes 501 and room key data 502 which are entered into the personal data device 10 from the hotel booking desk 521 and subsequently used to set the room lighting and heating 531 and operate the room lock 532 in a manner to be described.

Fig. 7 shows examples 601-605 of car data 240 which may obtained, for example, from the user's car manufacturer or dealer 621 and stored in the data store 11 of the personal data device 10 and subsequently used to operate locks 631, a car alarm 632 or other accessories 633. In addition data 604, 605 may be downloaded from the respective manufacturers 622, 623 of doors 634 and gates 635 so that they may be operated from the personal data device.

Similarly, Fig. 8 shows corresponding home data 250 which may be stored, such as door key codes 701, alarm codes 702 and heat, light, audio and video codes 703 that may be downloaded, for example, from a house agent or corresponding manufacturer 721, 722 and subsequently used to operate the corresponding devices 731-733.

A further example of a data grouping is so-called information data and software 260 shown in Fig. 9. This may include such semi-permanent updatable data as an address book 801, a business card 802, an appointments diary 803, bank details 804, insurance details 805, a donor card 806 and the user's medical history 807. This data group may include a copy of the current version of software 808 used on the personal data device so that this software may also be protected as well as the data in a manner to be described.

The method of operation of the personal data storage and protection system in its most general form is shown in the flowchart of Fig. 10. Referring also to Fig. 2, the personal data device 10 may have the functions of a known mobile telephone or a digital personal organiser, but is further provided with an authentication module 17 such as a fingerprint, iris pattern, voice recognition,

personal identity number or other authentication protection. On first use of the device the user's fingerprint or iris pattern, for example, are registered by the device in a manner known, *per se*. On subsequent attempts to access the personal data stored in the personal data device 10, step 910, the fingerprint, iris pattern or voice print, for example, is compared with the registered pattern to determine whether the user is registered to access to the stored data. A timing function may be provided to prevent access to the personal data after a user-variable period of non-use.

As shown in Fig. 2, associated with the personal data device 10 is a database server 50 having a database data store 51 in which can be stored a copy of the data to be stored in the personal data device. Preferably the database server includes encryption/decryption facilities so that the personal data may be stored in an encrypted format. The database server 50 may conveniently be a server connected to the Internet 30. In this case it is possible for the personal data device to communicate with the server over a mobile telephone link 21 from the mobile telephone compatible transmitter/receiver 14 in the personal data device to access the Internet 30. On first logging into the personal data device 10, it is therefore necessary to log into and register the personal data device with the Internet database server 50. This registration, as well as submitting usual identification data includes transmitting to the database server the registered fingerprint or iris pattern or other authentication data registered in the personal data device for a purpose described below. The data stored on the database server is protected in known ways from unauthorised access, preferably including password protection and encryption to at least a standard set by national or international standards bodies. Arrangements may be made to pay a registration fee on registering with the database server. On registration, the database server may download to the personal data device such additional software as is necessary to operate the invention, and an authentication code in the case of a device incorporating a smart card or SIM card, an element of the code being stored in the memory of the device and an element of the code being stored on the smart card. In this manner, the personal data stored in the device having a smart card can be protected in such a way that the personal data carried can only be accessible when the correct smart card is installed. This smart card can be used to store, for example, electronic

signatures for use in a manner to be described. Since the same or compatible authentication codes are downloaded to each of the users' devices, the downloadable software can be used in such a manner that access is only given to personal data stored on the devices from other devices having a compatible authentication code. In one embodiment of the invention, the software may be written in the JAVA language and the smart card may be a JAVA smart card, to take advantage of open standards and protocols.

The operation of the synchronisation authentication code is best illustrated by Fig. 1B. On switching on the mobile telephone, the data protection software compares, step 1001, the element 162 (see Fig. 1A) of the authentication, or jigsaw, code in the mobile telephone processor 16 with the element 195 of the authentication, or jigsaw, code stored on the smart card 19. If there is no code on the smart card or the code on the smart card does not correspond with that stored in the telephone, the data protection software initiates deletion, step 1040, of the protected personal data and/or any electronic signatures stored in the mobile telephone memory 11 and any protected personal data or electronic signatures stored in the smart card memory 193. In addition, the data protection software may notify the service provider to disable, step 1050, normal operation of the telephone. Thus if the device is stolen, and the smart card replaced, the device will not function with the replaced smart card because the codes do not match, nor can the device be operated with the existing smart card because the service provider has withdrawn service. If the codes in the telephone and the smart card do match then normal processing is resumed, step 1060, and on the user attempting to access protected personal data the telephone requests login input, as described below and best illustrated in Fig. 11. Such login input may be, for example, a Personal Identification number, a fingerprint pattern, an iris pattern or a voice pattern or any combination of these.

Although the invention has been described in relation to a mobile telephone, it will be apparent that the invention has equal applicability to, and a similar mode of operation in, the protection of data on, for example, a personal data administrator (PDA), a laptop computer and a personal computer. In the case

of, for example, a personal computer, it is possible in an embodiment of the invention, to nominate which files or folders are to be protected.

It is necessary to populate the personal data device with personal data to be protected. This may be conveniently performed, in part, using the Internet connection, as shown in Fig, 10, by accessing, step 920, an issuing authority and downloading data, step 940, after suitable authentication, step 930. For example, referring to Fig. 4, data normally stored on a debit card can be downloaded, step 940, to the personal data device to be stored as bank debit card data 301 by connecting the personal data device using the mobile telephone link 21 to the Internet 30 and then accessing a bank's server 321.

Alternatively, if the bank server, or a terminal connected to the server, is equipped with short-range wireless communications facilities using the same protocol, such as Bluetooth, which is used by the short-range transmitter/receiver 12 of the personal data device, then the data can be downloaded onto the device using the short-range wireless link 71 when the personal data device is within range of the bank server's transmitter/receiver.

In a similar manner electronic cash 302 or traveller's cheques 303 can be downloaded into the personal data device either using the Internet 30 or by using a Bluetooth equipped terminal similar to a known Automatic Teller Machine, and the user's bank account debited.

In addition, credit card data 304 and store card data 305 can be downloaded from a credit company server 322, preferably including the user's current credit limits. Alternatively, the device may include facilities for checking the status of the user's account on demand.

Gift voucher data 306 may be entered into the data store 11, for example, when received from, or on the instructions of, a donor by email.

With such data loaded in the personal data device the user may use the personal data device to make payments, for example at retail outlets such as shops and restaurants. In order for the user to be able to make payments the retail outlet is equipped with a point of sale terminal 331 having short-range wireless

communications functionality using the same communications protocol as the personal data device, for example, the Bluetooth protocol. In logging into the personal data device the user is identified as an authorised user by the fingerprint, iris pattern or other authentication module 17. This prevents the device being fraudulently used to make payments by an unauthorised user. A communications link 71 is then established, step 950, Fig. 10, between the point of sale terminal and the personal data device. The cost of the transaction is communicated to the personal data device from the point of sale terminal, the user selects a method of payment, for example by credit card, debit card or electronic cash, and authorises the payment. The user's data record is debited with the corresponding amount and, for example, if credit card payment has been selected, the user's credit card details 304 are uploaded, step 960, Fig. 10, to the point of sale terminal 331 and the retailer's account subsequently credited by obtaining a refund from the credit company or bank in a known manner, step 970. Where required, the transaction may be further authenticated by an electronic signature. Alternatively, electronic cash, for example, may be transferred from the personal data device to the transaction terminal.

If the personal data device credit card data also includes the user's current credit limit, there is no requirement for the retailer to receive authorisation from the credit card company before accepting payment since a credit check can be carried out directly with the personal data device. In addition, the user's available credit limit in his personal data device can be immediately debited by the value of the transaction to indicate the user's new available credit limit. The current value of credit available will obviously be raised again when the user next makes a payment to the credit card company, in a manner to be described. When the user makes credit card payments, other than by using the personal data device, the available credit limit may also be updated by the credit card company by updating the personal data on the database server so that the corresponding data on the personal data device may subsequently be updated.

The personal data device may also hold many other types of data as illustrated in Fig. 4. For example, personal identification data 307, or passport data 308 downloaded from a passport issuing authority 323, in an analogous manner to

that in which the monetary data is downloaded. Such data would typically include a passport-type photo of the authorised user. The personal data device may then be used at, for example, an airport check-in desk or a port of entry 332 to communicate with a Bluetooth-equipped terminal so that the passport data, including the stored photograph, may be displayed to an operator or used in, for example, automatic validation or immigration checks without any requirement for the operator to key in the data.

As illustrated in Fig. 4, the stored data may also include social security data 309 downloaded from Social Security authorities 324 and used for example for claiming benefit at benefit offices 333. Such payments could be in the form of electronic cash 302 paid into the personal data device. Similarly, driving licence data 310 may be downloaded from a driving licence authority 325 and read automatically by, for example, police officers equipped with Bluetooth compliant equipment 334, again without the delay or possibility of error associated with the data being keyboarded by a remote police operator. In another application, membership details may be downloaded from, for example, a club or society Internet website automatically to grant the user privileges of membership when the user's device is read by Bluetooth compliant equipment 335. International calling card data 312 may also be held with the fixed data 210.

Referring to Fig. 5, the personal data device can also be used to store less permanent or temporary data 220. For example, the device may store ticket details 401, for example for transport or entertainment. Thus, a train season ticket or airline ticket may be bought online over the Internet 30 using the device's mobile telephone facilities 14 or from a booking office using the short-range wireless link 71. The device then may be used to gain entrance through a ticket barrier 431 that is, for example, Bluetooth-compliant. Similarly, boarding pass data 402 can be downloaded over the Bluetooth-compliant wireless link 71 at an airport check-in desk 422 and then read, and if required, deleted, at a Bluetooth-compliant equipped boarding gate 432. In addition, prescription data 403 can be downloaded at a doctor's or optician's surgery 423 using Bluetooth-compliant terminal and read and if required deleted using another Bluetooth-compliant terminal 433 at a pharmacy or dispensing optician respectively. Alternatively, if a medical

condition is diagnosed by a doctor from a location remote from a patient, or for repeat prescriptions, the prescription may be downloaded to the patient's device using the Internet 30.

As shown in Fig. 6, the invention also has application in an hotel environment. On booking into the hotel at a check-in desk 521 a code for an assigned room key 502 may be downloaded into the personal data device 10 and then the data used to unlock and lock the room door 532 by transmitting the stored code to the door lock using another Bluetooth compliant wireless link 71. Similarly, room setting codes 501 may be downloaded to allow the device to be used remotely to control the room lighting and heating 531, for example. In an embodiment of the invention, the device may establish a communication link 71 with the remote light control, for example, when the device comes within range of the control and cause the display of an icon depicting the light switch on a display of the personal data device. As an alternative to the data being loaded at the hotel check-in desk 521, where a room is booked in advance, time-limited data may be downloaded remotely, using, for example, the Internet 30, into the user's personal data device, thereby hastening checking in, or avoiding the need to check in on arrival. Where the data is not time-limited, so that the data 230 is not automatically deleted from the personal data device at the end of the booked stay, the data may be deleted as part of the checking-out procedure.

As shown in Fig. 7, the invention also has application in relation to data 240 related to use of a car. In a manner analogous to the hotel application the personal data device may be used to store key codes 601, alarm codes 602 and codes 603 for the operation of such accessories as heating, audio, seat adjustment and navigation controls. These codes may, for example, be remotely downloaded from the car or accessory manufacturer's server 621 or downloaded locally or remotely from a car dealer. Alternatively, where new accessories are added to a car, they may be supplied with a barcode or other machine-readable device for entering the code 603 into the personal data device. In an analogous manner, codes 604,605 may be downloaded from respective manufacturers 622, 623 for operating a remotely controlled garage door 634 or a gate 635. Alternatively, the

codes may be stored in an in-car computer and accessed using an electronic signature stored in the personal data device.

The system of the invention also has application for data 250 used in a home, as illustrated in Fig. 8, in a manner analogous to that of the car in that key codes 701, alarm codes 702 and other remote control codes 703 can be stored by, for example, downloading from the corresponding manufacturer or house agent 721, 722 and used to operate Bluetooth-compliant locks 731, alarms 732 and other devices 733. When the personal data device is brought within range of a Bluetooth terminal in the user's home, the device may initiate the turning on of lights, and setting heating to a predetermined temperature.

Referring to Fig. 9, the personal data device may also be used to store other variable data 260, in a known manner, which may, for example, be entered from a keyboard, or downloaded from a personal computer 60 in a manner to be described. Thus the device may incorporate an address book 801, an appointments diary 803 as well as a business card 802, which may be emailed over the Internet 30 or transmitted by a Bluetooth link 71 to another personal data device. The device may also be used to store, for example, insurance details 805, donor card data 806 and the user's medical history 807. It will be appreciated that the medical history may then be read and updated in any medical consultation, intervention or emergency by Bluetooth-compliant equipment.

Facilities may be provided for emergency access to the medical history data, which bypasses the authentication facilities, for use when the authorised user is unconscious or otherwise incapacitated.

Alternatively, in a number of applications, instead of personal data being stored on the personal data device, an electronic signature may be stored on the personal data device to give access to personal data stored on another device or computer.

As indicated above, and referring again to Fig. 2, the personal data device is also connectable, for example using the Internet 30, to a database server 50 having a database data store 51 for storing a copy of the data stored in the data store 11 of the personal data device 10. The database server may thus be used to

store a duplicate version of the data and software stored in the personal data device. It is therefore necessary for the personal data device to be logged into the database server from time to time to synchronise the data stored on the personal data device and on the database server. For example, the personal data device may contact the database server 50 over the internet 30 every time an amendment or addition is made to the personal data stored on the personal data device. Alternatively, updates may be made after, say, every three changes or at some other frequency chosen by the user. Facilities may be provided on the database server to compare the version of the personal data already stored with the current data in the personal data device and only to copy in either direction, as appropriate, any data which has changed or is new on either the device or the server, to create new current versions on both the device and the server.

This two-way checking is necessary because the database server may also be used to store updates from the issuing authorities, for example, a new available credit limit when a payment is made by the user to the credit card company or when credit card payments are made other than by the personal data device, so that the personal data device may be updated with the new data when the device 10 is next logged into the database server 50.

An authorised user may view his or her personal data stored on the personal data device or on the database server, subject to authorisation. The data may have associated internet addresses of the corresponding issuing authorities, so that a user may, for example, access the issuing authority server to access the user's details or account on the issuing authority server.

The database server also performs an important function when a personal data device is missing or replaced. Referring to Fig.12, if a personal data device 10 is reported missing, step 110, to the database server 50, the database server seeks to contact the missing device. The device may, for example, be reported missing by contacting the database server via the Internet or telephone. The database server preferably contacts the device in a manner undetectable to a user, for example, by sending a SMS message. Either when the device is next switched on or, alternatively, the personal data device may be provided with sufficient functionality even when nominally powered off to receive the SMS message and

act upon it. Such functionality may be powered by a main battery of the personal data device or by an auxiliary standby battery. The standby power also powers a reset 193 for a purpose to be described. An icon may be displayed on the personal data device display when the device is powered off to indicate that the data is protected by being duplicated on the database server. On being notified that the personal data device is no longer in the possession of the authorised user, the database server compares the data stored in the personal data device with that stored for that device in the database and, if appropriate, updates the version stored in the database using the data stored in the personal data device. The database server then signals the personal data device to delete, step 111, the data and/or any electronic signatures held in the personal data device so that the data cannot be used by an unauthorised user, for example, by using the reset facility 193 to reset all variables stored in the personal data device to default values. Moreover, the database server does not authorise subsequent registration of the personal data device with the database server, except by the authorised user. Therefore, even if an unauthorised user manages to bypass the fingerprint or other authentication facility incorporated in the personal data device, the device provides only limited functionality to the unauthorised user. In addition, the data store 11 of the personal data device may be designed to be sufficiently volatile that should a thief remove the power supply to prevent a "silent call" deleting the stored data, the stored data and/or any stored electronic signatures will be automatically deleted and, for example, all variables reset to default values when the power supply is restored. The database server may also contact all issuing authorities to inform them that the device is missing, so that the issuing authorities may, if desired, issue new account numbers, codes or other details for subsequent use by the authorised user on a replacement personal data device. For this purpose, the issuing authority may, after suitable authentication, download the new data into the user's data on the database server to be subsequently downloaded to the user's replacement personal data device.

The authorised user can replace the missing personal data device, or upgrade to a later model, and after initialising, step 112, the new device, can log into the database server 50, step 113, and download, step 114, all the user's duplicate data from the database server onto the new personal data device. In

order to download the data it is necessary to enter the authorised user's name and password. If the user has forgotten his or her access information the user may, for example, contact a server operator by selecting an icon on the database server website and answer identifying questions either by voice or text communication, in order to obtain access to his or her personal data. The database server will provide an opportunity to remind the user of the registered name and password before the user logs off. Alternatively, where pattern recognition is employed to identify authorised users, this will provide access to the user's personal data on the server either through the user's personal data device or a personal computer, provided the pattern is also stored on the database server. In this manner the user can replace a device and reload the device with data using the Internet, wherever the user may be in the world.

As a further refinement, a facility may be provided on the database server, following a report of a loss of a personal data device, either to despatch a replacement directly to the user or to authorise a local supplier to issue a replacement device to the user. Such a service may be covered by insurance.

As shown in Fig. 11, in an embodiment of the invention, the device may be further protected by automatic deletion of the data stored in the personal data device on failure successfully to log into the personal data device after, for example, a second attempt. Thus, the user makes a first attempt to log into the device, step 1000, and if successful is presented, step 1010, with a device main menu. If unsuccessful, a second attempt, step 1020, may be made and if successful the main menu is presented, step 1010. However, if logging in is unsuccessful at the second attempt the device deletes, step 1040, all the data and/or any electronic signatures in the personal data device. Preferably, before deleting the data, the device contacts the database server 50 and uploads, step 1030, at least any data to the database server that is necessary to create a current backup. An authorised user may, subject to proper authentication, subsequently reload the data from the back-up into the personal data device. In a similar manner, the data and/or any electronic signatures will be deleted if an attempt is made to read personal data using an incompatible authentication code.

In an embodiment of the invention, access is provided to the database server 50 from a user's personal computer 60, as shown in Fig. 2. The user may then maintain a copy of the data stored in the personal data device in a data store 61 of the personal computer. Alternatively, a personal computer could be used to keep the only backup of the personal communications data, without the use of a database server and the personal computer used for all the functions otherwise carried out by the database server. In an embodiment of the invention, where the personal computer is equipped with short-range wireless communications facilities, communication between the personal data device and the personal computer may, in addition or alternatively, be by a short-range wireless link.

Moreover, the feature of protection of data by the use of an authentication code and protection software downloaded from a module such as a smart card, so that an element of the code is stored in the device memory and an element of the code stored on the smart card, to prevent operation of the device, or access to personal data or electronic signatures stored in the personal data device, unless the original smart card is installed, may be used without, or independently, of the feature of maintaining a copy of the personal data or electronic signature on another computer such as a PC or Internet server.

CLAIMS

1. A personal data device including: data storage means for storing data including at least one of personal data and at least an element of an electronic signatures, access authentication means for restricting access to said data stored in the data storage means to an authorised user, a data storage and processing module for enabling operation of the personal data device, data protection software and a synchronisation authentication code, at least a first element of the code being stored in the data storage means and at least a second element of the code being stored in the data storage and processing module, such that, when the at least a first element of the code stored in the data storage means and the at least a second element of the code stored in the module correspond, access is allowed by the data protection software to said data and, when the at least a first element of the code stored on the module and the at least a second element of the code stored in the data storage means do not correspond, the said data stored in the data storage means are deleted by the data protection software.

2. A personal data device as claimed in claim 1, wherein the device further includes first communication means for downloading the data protection software and the synchronisation authentication code from a remote server.

3. A personal data device as claimed in claims 1 or 2, wherein the data protection software and the synchronisation authentication code are downloadable from the data storage and processing module.

4. A personal data device as claimed in claim 2, wherein the first communication means is also for communicating with the remote server or another computer device for transmitting a copy of the personal data to the remote server or other computer device such that synchronisation of the personal data with data stored on the remote server or other computer device is permitted by the data protection software dependant upon authentication with the remote server or other computer device using at least an element of the synchronisation authentication code.

5. A personal data device as claimed in any of claims 2 to 4, wherein at least one of personal data and at least an element of an electronic signature may also be stored in the data storage and processing module.

6. A personal data device as claimed in any of claims 2 to 5, wherein the access authentication means permits access to the personal data in response to a predetermined input and in response to consecutive inputs a predetermined number of times of inputs other than the predetermined input the data protection software deletes said data stored in the data storage means and in the data storage and processing module.

7. A personal data device as claimed in any of claims 2 to 6, wherein the access authentication means includes pattern recognition means.

8. A personal data device as claimed in claim 7, wherein the pattern recognition means is for recognising at least one of the authorised user's fingerprint pattern, iris pattern and voice pattern.

9. A personal data device as claimed in any of the preceding claims, wherein the data storage and processing module is removable from the personal data device.

10. A personal data device as claimed in any of the preceding claims, wherein the data storage and processing module is a smart card.

11. A personal data device as claimed claim 6, wherein the personal data device includes deletion means under control of the data protection software for deleting said data stored in the data storage means and in the data storage and processing module when an input to the access authentication means does not match the predetermined input.

12. A personal data device as claimed in claim 11, wherein the deletion means is also for deleting the said data, under control of the data protection software, on receipt of a deletion signal from the remote server.

13. A personal data device as claimed in claim 12, wherein the deletion signal from the remote server is an SMS message.

14. A personal data device as claimed in claims 12 or 13, wherein the personal data device is provided with uninterruptible standby power supply means sufficient to power the first communication means for reception of the deletion signal and to power the deletion means to delete the said data.

15. A personal data device as claimed in any of claims 11 to 14, wherein the deletion means is also for resetting variables stored in the personal data device to default values.

16. A personal data device as claimed in claim 4, wherein the personal data device includes means for establishing communications with the remote server to synchronise personal data stored in the data storage means with personal data stored on the remote server after a predetermined number of additions or amendments to the stored data have been made.

17. A personal data device as claimed in any of the preceding claims, wherein encryption means are provided for encrypting the personal data for storing the personal data in the personal data device in an encrypted form.

18. A personal data device as claimed in any of the preceding claims, wherein the personal data device further includes second communication means for transferring at least some of the stored personal data between the personal data device and a transaction terminal.

19. A personal data device as claimed in claim 18, wherein the first communication means is for connection to a mobile communications network and the second communication means is a short-range wireless communication means.

20. A personal data device as claimed in claim 19, wherein the short-range wireless communication means is adapted to operate over a range up to 100 metres.

21. A personal data device as claimed in claims 18 or 19, wherein the personal data device storage device includes display means and the device is adapted to display appropriate menu items or icons on the display means dependent on detection of a signal transmitted from a transaction terminal within range of the short-range wireless communication means.

22. A personal data device as claimed in any of the preceding claims, wherein the personal data device data storage means is for storing fixed data updatable only by a corresponding issuing authority and for storing user data updatable by the authorised user.

23. A personal data storage device as claimed in claim 22, wherein the personal data device data storage means is for storing data corresponding to any one or more of a credit card, a debit card, a passport and social security data .

24. A personal data storage device as claimed in claims 22 or 23, wherein the personal data device data storage means is for storing electronic cash and/or travellers' cheques.

25. A personal data storage device as claimed in any of claims 22 to 24, wherein the personal data device data storage means is for storing temporary data updatable by an issuing authority, including any one or more of tickets, boarding passes, prescriptions and hotel room access keys.

26. A personal data storage device as claimed in any of claims 22 to 25, wherein the personal data device data storage means is for storing data relating to the authorised user's home and/or car, including any one or more of access keys, alarm control, automatic door and gate control.

27. A personal data storage device as claimed in any of claims 22 to 26, wherein the personal data device data storage means is for storing user-updatable data including any one or more of address book entries, business cards, appointment diary, bank details, insurance details, donor card and medical history.

28. A database server including: server data storage means; downloadable data protection software and an authentication code generator; and server communication means for downloading to first communication means on a personal data device, the personal data device also including data storage means for storing personal data and a data storage and processing module for enabling operation of the personal data device, data protection software and a synchronisation authentication code for storing at least a first element of the code in the data storage means and at least a second element of the code in the data

storage and processing module, wherein the server communication means is also for receiving from the personal data device a copy of the personal data for storing in the server data storage means dependant upon authentication using the synchronisation authentication code, such that, when the first element of the code stored in the module and the second element of the code stored in the data storage means correspond, access is allowed by the data protection software to the personal data and synchronisation of the personal data with personal data stored on the server is permitted by the data protection software and, when the first element of the code stored on the module and the second element of the code stored in the data storage means do not correspond, the personal data and/or any elements of electronic signatures stored in the personal data device data storage means is deleted by the data protection software.

29. A database server as claimed in claim 28, wherein the database server includes data comparison means for comparing a first version of the personal data uploaded from the personal data device and a second version of the personal data stored in the server data storage means and means to extract a current version of the data from the first version and the second versions from which to form a synchronised version to replace the data stored on both the personal data device and the database server.

30. A database server as claimed in claims 28 or 29, wherein the database sever includes encryption means and decryption means such that the personal data may be stored in the server data storage means in an encrypted format.

31. A database server as claimed in any of claims 28 to 30, wherein the database server is provided with signalling means to communicate with the personal data device to signal the data protection software to delete the personal data and/or any elements of electronic signatures in the personal data device data storage means.

32. A database server as claimed in claim 31, wherein the signalling means is for signalling the personal data device to delete the personal data and/or any elements of electronic signatures stored in the personal data device data storage

means on the database server being updated that the personal data device is no longer in the possession of the authorised user.

33. A database server as claimed in any of claims 28 to 32, wherein replacement means are provided to replace a personal data device that has been reported lost or stolen with a replacement personal data device into which the personal data stored on the database server may be reloaded.

34. A personal data protection system comprising:

a personal data device including data storage means for storing personal data, a processing and data storage module for enabling operation of the personal data device when a first element of a synchronisation authentication code stored in the module corresponds with a second element of the synchronisation authentication code stored in the data storage means, first communication means for connection of the personal data device to a communication network; and

a database server including server communication means connectable to the communications network for downloading a copy of the personal data stored in the personal data device to form copied data, server data storage means for storing the copied data, such that the data in the server data storage means and the data in the personal data device may be mutually updated and synchronised by communication over the communications network, downloadable data protection software for downloading to the personal data device and a synchronisation code generator for generating a synchronisation authentication code for downloading to the personal data device.

35. A system as claimed in claim 34, wherein the personal data device is further provided with short-range wireless communication means for communicating at least some of the personal data and the system is further provided with a transaction terminal having short-range wireless communication means for communicating with the short-range communications means of the personal data device for initiating a transaction by the transaction terminal.

36. A system as claimed in claims 34 or 35, wherein the system is further provided with an issuing authority server having issuing authority communication means for updating the personal data stored in the personal data device.

37. A system as claimed in claim 36, wherein the issuing authority server is connectable to the communications network for updating the personal data stored in at least one of the database server and the personal data device.

38. A system as claimed in claims 36 or 37, wherein the issuing authority server includes short-range issuing authority communication means for communicating with the personal data device short-range communication means for updating the personal data stored in the personal data device.

39. A method for storing and protecting personal data comprising the steps of:

a) providing a personal data device including: data storage means for storing personal data, first communication means for communicating over a communications network and a data processing and storage module for enabling operation, under control of data protection software, of the personal data device when a first element of a synchronisation code stored on the module corresponds with a second element of a synchronisation authentication code stored in the personal data device storage means;

b) storing personal data in the data storage means;

c) providing a database server connectable to the communications network for receiving from the personal data device and storing a copy of the personal data stored in the personal data device such that the personal data in the personal data device and the database server may be mutually updated and synchronised;

d) providing downloadable data protection software and a synchronisation authentication code generator on the database server;

e) downloading the data protection software and a synchronisation authentication code from the database server to the personal data device and loading a first element of the synchronisation authentication code in the data storage and processing module and a second element in the data

storage means of the personal data device such that operation of the personal data device is enabled;

f) providing deletion means in the personal data device for deleting, under control of the data protection software, the personal data and/or an element of an electronic signature stored in the data storage means when the first element of the synchronisation code does not correspond with the second element of the synchronisation authentication code or on receipt of a deletion signal from the database server.

40. A computer program comprising code means for performing all the steps of the method of claim 39 when the program is run on one or more computers.

41. A computer program as claimed in claim 40, wherein the computer program is embodied on a computer-readable medium.

42. A computer program product comprising program code means stored in a computer-readable medium for performing the method of claim 39 when that program product is run on one or more computers.

43. A personal data storage device substantially as herein described with reference to and as illustrated in the accompanying drawings.

44. A database server substantially as herein described with reference to and as illustrated in the accompanying drawings.

45. A system substantially as herein described with reference to and as illustrated in the accompanying drawings.

46. A method substantially as herein described with reference to and as illustrated in the accompanying drawings.

47. A computer program substantially as herein described with reference to and as illustrated in the accompanying drawings.

Application No: GB 0028154.3 33 **Examiner:** D Midgley
Claims searched: 1-47 **Date of search:** 21 December 2001

Patents Act 1977
Search Report under Section 17

Databases searched:

UK Patent Office collections, including GB, EP, WO & US patent specifications, in:

UK Cl (Ed.S): G4A AUXX,AAP

Int Cl (Ed.7): G06F 1/00,12/14,13/38 H04Q 7/32

Other: ONLINE:WPI,EPODOC,JAPIO US Class.:700/231,700/237,711/100,711/164

Documents considered to be relevant:

Category	Identity of document and relevant passage	Relevant to claims
A	US 6026293 (ERICSSON)	1,28,34 and 39

X	Document indicating lack of novelty or inventive step	A	Document indicating technological background and/or state of the art.
Y	Document indicating lack of inventive step if combined with one or more other documents of same category.	P	Document published on or after the declared priority date but before the filing date of this invention.
&	Member of the same patent family	E	Patent document published on or after, but with priority date earlier than, the filing date of this application.